Piloting a DDoS Clearing House for Europe

Cristian Hesselman (SIDN Labs)
CONCORDIA Open Door Event
Oct 17-18, 2019
Luxembourg City, LU
DDoS examples

Mirai botnet: Dyn, OVH (hosting provider), Krebs On Security (website), Deutsche Telecom (ISP)


January 2018
A few DDoS trends

• Volume at 1+ Tbps, likely going up (e.g., GitHub 1.3 Tbps)
• Many widely distributed sources (Mirai 600K, Hajime 400K)
• High propagate rates (e.g., Mirai from 42K to 71K bots in 1 hour)
• Complex traffic (e.g., bot churn, volumetric/TCP state exhaustion)
• Easier to launch through booters/stressers (Mirai)
• Reflection attacks possible (e.g., Mirai and Reaper botnets)
DDoS clearing house concept

- Continuous and automatic sharing of “DDoS fingerprints” buys providers time (proactive)

- Extends DDoS protection services that critical service providers use and does not replace them

- Improves attribution, allowing for better prosecution and increased deterrent effects
DDoS fingerprints = summary of DDoS traffic

- Examples: source IP addresses, port numbers, protocol type, no victim IP addresses

- Optional: PCAPs, device-specific packet filter rules, suspected type of DDoS attack (e.g., Mirai)

- Created from network measurements (e.g., PCAP, Netflow, IPFIX, sFlow, Logfile)

Source: [Conrads]
Clearing house architecture (draft)

• Key component: DDoS dissector

• Sharing within and across providers through fingerprint databases

• OPS teams in control
  – Outgoing: filtering of fingerprints
  – Incoming: writing and installing filtering rules based on fingerprints

https://github.com/ddos-clearing-house
Pilot in the Netherlands

• Joint effort 10 different orgs (including 3 CONCORDIA partners)

• Iteration 1: set up full “fingerprint sharing cycle” (tech + legal)

• Iteration N>1: iteratively improve clearing house
  – Improve Dissector (e.g., add API and signing of fingerprints)
  – Optionally add more partners
  – Update data sharing agreement
Status NL pilot

- Inter-domain DDoS-DB running at SIDN Labs

- Key challenge: data sharing agreement clearing house
  - Draft available, developed by KPN and SIDN
  - Legal folks finalizing loose ends
Iteration 1 data sharing agreement

• Requirement #1: simple
  – Minimal # topics (e.g., objective, liability, security, PII, governance)
  – DDoS fingerprints only include metadata for now, no PCAPs
  – Fixed but extensible duration of 6 months

• Requirement #2: scalable
  – Parties: SIDN (DDoS-DB operator) and KPN (test member)
  – KPN as ”more complex” partner (larger company, regulation)
  – Translate to English for use in CONCORDIA
Broader view: Dutch anti-DDoS coalition

Objective: further improve the protection of Dutch critical services by sharing expertise, experiences, and operational data on DDoS attacks

Working groups:
- Clearing house
- Emergency exercises
- Outreach
- Ground rules and incident response
- Sustainable collaboration

Reinforced DDoS resilience of Dutch critical services
Lessons learned in NL so far

• Overall observations
  – Need for a DDoS clearing house widely acknowledged
  – Other gaps: DDoS exercises and sharing experience and expertise
  – Personal trust has been key at this stage

• Data sharing agreement
  – Close collaboration between legal and tech from the start is a must
  – Provide guidance for legal experts on concept of DDoS fingerprints
  – Legal uncertainty may lead to conservatism (cf. [daSilva])
  – Find level of simplicity and scalability that matches pilot iteration
Partners in NL

SIDN, SURFnet, and the University of Twente were partly funded by the European Union's Horizon 2020 Research and Innovation program under Grant Agreement No 830927.
Proposed next steps T3.2

- Pilot NL: finalize data sharing agreement, request NL partners to sign, share via DDoS-DB at SIDN Labs, start improving the software

- Research: set up DDoS-DB for T3.2, request T3.2 partners to sign data sharing agreement, start sharing fingerprints, run experiments (e.g., clustering of fingerprints, rule generation) and write the cookbook

- Feed research results back into the NL pilot as well as into IT pilot

- Partners: SIDN, SURF, TI, UT, CODE, UZH, Ericsson
Contact
Research Institute CODE
Carl-Wery-Straße 22
81739 Munich
Germany
contact@concordia-h2020.eu

Follow us
www.concordia-h2020.eu
www.twitter.com/concordiah2020
www.facebook.com/concordia.eu
www.linkedin.com/in/concordia-h2020
www.instagram.com/concordiah2020.eu

Q&A
Cristian Hesselman (T3.2 lead)
cristian.hesselman@sidn.nl
@hesselma
+31 6 25 07 87 33
Further reading


